Averages of elliptic curve constants

Nathan Jones

jones@dms.umontreal.ca

Abstract

We compute the averages over elliptic curves of the constants occurring in the Lang-Trotter conjecture, the Koblitz conjecture, and the cyclicity conjecture. The results obtained confirm the consistency of these conjectures with the corresponding "theorems on average" obtained recently by various authors.

1 Introduction

Let E be an elliptic curve defined over the rational numbers and for a prime p of good reduction for E, let E_p denote the reduction of E modulo p. There are various conjectured asymptotics for functions which count good primes p up to x for which the reduced curve E_p has certain properties. In this paper we will focus on three such questions, although our methods are applicable to a wider range of problems. For a fixed integer r, let

$$\pi_{E,r}(x) = |\{p \leq x : p \nmid \Delta_E,\ a_p(E) = r\}|,$$

where $a_p(E) = p + 1 - |E_p(\mathbb{Z}/p\mathbb{Z})|$ is the trace of the Frobenius endomorphism of E at p. Lang and Trotter [13], using a probabilistic model consistent with the Chebotarev density theorem and the Sato-Tate conjecture, predicted an asymptotic for $\pi_{E,r}(x)$:

Conjecture 1. *(Lang-Trotter) Assume that either E has no complex multiplication or that $r \neq 0$. Then*

$$\pi_{E,r}(x) \sim C_{E,r}\frac{\sqrt{x}}{\log x} \qquad \text{as } \ x \to \infty,$$

where $C_{E,r}$ is a specific constant.

We will describe the constant $C_{E,r}$ in detail in section 3. The second conjecture we will consider involves the counting function

$$\pi_{E,\text{prime}}(x) := |\{p \leq x : p \nmid \Delta_E,\ |E(\mathbb{Z}/p\mathbb{Z})| \text{ is prime }\}|.$$

Conjecture 2. *(Koblitz)*

$$\pi_{E,prime}(x) \sim C_{E,prime}\frac{x}{(\log x)^2} \qquad as \;\; x \to \infty,$$

where $C_{E,prime}$ is a specific constant.

Finally we will consider the cyclicity conjecture, which has been settled conditionally by Serre [17] and unconditionally in the CM case by Murty [14] and also by Cojocaru [4]. Let

$$\pi_{E,\mathrm{cyclic}}(x) := |\{p \le x : p \nmid \Delta_E,\ E(\mathbb{Z}/p\mathbb{Z}) \text{ is a cyclic group }\}|.$$

Conjecture 3. *(Cyclicity conjecture)*

$$\pi_{E,cyclic}(x) \sim C_{E,cyclic}\frac{x}{\log x} \qquad as \;\; x \to \infty,$$

where $C_{E,cyclic}$ is a specific constant.

Recently, various authors have proven that these conjectures "hold on average over elliptic curves." More precisely, for parameters $A = A(x)$ and $B = B(x)$, let $\mathcal{C} = \mathcal{C}(x)$ denote the set of elliptic curves $Y^2 = X^3 + aX + b$ with $(a, b) \in ([-A, A] \times [-B, B]) \cap \mathbb{Z}^2$. Fouvry and Murty [8] (in case $r = 0$) and later David and Pappalardi [6] (in case $r \neq 0$) proved Conjecture 1 on average: for any $\varepsilon > 0$, if $\min\{A(x), B(x)\} \ge x^{1+\varepsilon}$ then

$$\frac{1}{|\mathcal{C}(x)|}\sum_{E\in\mathcal{C}(x)} \pi_{E,r}(x) \sim C_r\frac{\sqrt{x}}{\log x}, \quad \text{as } x \to \infty, \tag{1}$$

where C_r is a specific constant. S. Baier [1] has recently shortened the length of the average, replacing "$x^{1+\varepsilon}$" with "$x^{3/4+\varepsilon}$."

Balog, Cojocaru and David [2] have proved a similar average theorem for Conjecture 2: for any $\varepsilon > 0$, if $\min\{A(x), B(x)\} \ge x^{1+\varepsilon}$ then

$$\frac{1}{|\mathcal{C}(x)|}\sum_{E\in\mathcal{C}(x)} \pi_{E,\mathrm{prime}}(x) \sim C_{\mathrm{prime}}\frac{x}{(\log x)^2}, \quad \text{as } x \to \infty, \tag{2}$$

where C_{prime} is a specific constant.

Finally, Banks and Shparlinski [3] have proved Conjecture 3 unconditionally on average: for any $\varepsilon > 0$, if $x^{2/3+\varepsilon} \le A(x), B(x) \le x^{1-\varepsilon}$ then

$$\frac{1}{|\mathcal{C}(x)|}\sum_{E\in\mathcal{C}(x)} \pi_{E,\mathrm{cyclic}}(x) \sim C_{\mathrm{cyclic}}\frac{x}{\log x}, \quad \text{as } x \to \infty, \tag{3}$$

where C_{cyclic} is a specific constant.

In this paper we will prove that each of these average results is consistent with the corresponding conjectured result on the level of the constants. We will make the notation uniform.

Notation 4. *Throughout the rest of this paper, let C_E denote any one of the constants $C_{E,r}$, $C_{E,prime}$, or $C_{E,cyclic}$, and let C denote the corresponding average constant C_r, C_{prime}, or $C_{E,cyclic}$.*

Our first theorem is conditional upon an affirmative answer to the following question of Serre [16]. In its statement, $\mathbb{Q}(E[p])$ denotes the p-th division field of E, i.e. the field obtained by adjoining to $\mathbb{Q}$ the x and y-coordinates of a given Weierstrass model of E.

Question 5. *Does there exist an absolute constant c so that, for any prime $p > c$ and any elliptic curve E over $\mathbb{Q}$ one has*

$$Gal(\mathbb{Q}(E[p])/\mathbb{Q}) \simeq GL_2(\mathbb{Z}/p\mathbb{Z})?$$

We prove

Theorem 6. *Assume that Question 5 has an affirmative answer. Then for any positive integer k and any $\varepsilon > 0$, we have*

$$\frac{1}{|\mathcal{C}|}\sum_{E\in\mathcal{C}} |C_E - C|^k \quad \ll_{k,\varepsilon} \quad \max\left\{\left(\frac{A^\varepsilon \log B}{B}\right)^{\frac{k}{k+1}}, \frac{\log^{3k+\gamma}(A^3+B^2)}{\sqrt{\min\{A,B\}}}\right\}.$$

Note the following

Corollary 7. *Provided that Question 5 has an affirmative answer and that, for some $\varepsilon > 0$, $A^\varepsilon \ll B \ll e^{A^{\frac{1/2-\varepsilon}{3+\gamma}}}$, then as $A \to \infty$, one has*

$$\frac{1}{|\mathcal{C}|}\sum_{E\in\mathcal{C}} C_E \ \longrightarrow\ C$$

Taking $k = 2$, we also note the following corollary to Theorem 1.4 of [6], which bounds the average error in the Lang-Trotter conjecture.

Corollary 8. *Let $\varepsilon > 0$ and $c > 0$ be given and suppose that Question 5 has an affirmative answer. Then, provided that $A, B > x^{2+\varepsilon}$ and that*

$$\max\left\{\left(\frac{A^\varepsilon \log B}{B}\right)^{\frac{2}{3}}, \frac{\log^{6+\gamma}(A^3+B^2)}{\sqrt{\min\{A,B\}}}\right\} \ \ll\ \frac{1}{(\log x)^{c-2}},$$

one has

$$\frac{1}{|\mathcal{C}|}\sum_{E\in\mathcal{C}} \left|\pi_{E,r}(x) - C_{E,r}\frac{\sqrt{x}}{\log x}\right|^2 \ll \frac{x}{(\log x)^c}.$$

Unconditionally, we prove a statement about averages over Serre curves (we will review the notion of a Serre curve in Section 4).

Theorem 9. *Let k be a positive integer. For each $\varepsilon > 0$, we have*

$$\frac{1}{|\mathcal{C}|}\sum_{\substack{E\in\mathcal{C}\\ E \text{ is a Serre curve}}} |C_E - C|^k \quad \ll_{k,\varepsilon} \quad A^\varepsilon \cdot \left(\frac{\log B}{B}\right)^{k/(k+1)}.$$

Because of the fact that

$$\frac{1}{|\mathcal{C}|} \sum_{\substack{E\in\mathcal{C}\\ E \text{ is a Serre curve}}} 1 \quad \longrightarrow \quad 1$$

as $\min\{A,B\} \to \infty$ (c.f. [10]), Theorem 9 provides evidence that Theorem 6 should hold unconditionally.

2 Acknowledgments

I wish to thank W. Duke for bringing this problem to my attention and also C. David and A. Granville for comments on an earlier version.

3 The constants

In this section we will describe precisely the constants occuring in the conjectures under consideration, as well as the corresponding average constants. Their description involves the division fields of E, whose notation we now fix.

Notation 10. *For each positive integer n, denote by $\mathbb{Q}(E[n])$ the n-th division field of E, obtained by adjoining to $\mathbb{Q}$ the x and y-coordinates of the n-torsion of E, and by*

$$G_n(E) := Gal(\mathbb{Q}(E[n])/\mathbb{Q})$$

the associated Galois group. Since $E[n]$ is a free $\mathbb{Z}/n\mathbb{Z}$-module of rank 2, we may (by fixing a $\mathbb{Z}/n\mathbb{Z}$-basis) view $G_n(E)$ as a subgroup of $GL_2(\mathbb{Z}/n\mathbb{Z})$.

We will distinguish between the case where E has complex multiplication (CM) and the case where E does not (non-CM). Since almost all elliptic curves are non-CM [7], our only interest in the CM case is to obtain upper bounds for C_E.

3.1 The CM case

Suppose that E has complex multiplication by an order $\mathcal{O}$ in an imaginary quadratic field K. Let w be the number of roots of unity in K and Δ_K the discriminant of K.

Then, as computed in [13, pp. 87–88], we have

$$C_{E,r} = \frac{w}{2\pi}\cdot F_4(r,K)\cdot \prod_{\substack{\ell\neq 2\\ \ell\mid\Delta_K}} \frac{\ell}{\ell-1}\cdot \prod_{\substack{\ell\neq 2\\ \ell\nmid\Delta_K\\ \ell\mid r}} \frac{\ell}{\ell-\left(\frac{\Delta_K}{\ell}\right)}\cdot \prod_{\substack{\ell\neq 2\\ \ell\nmid\Delta_K\\ \ell\nmid r}} \left(1-\frac{\left(\frac{\Delta_K}{\ell}\right)}{(\ell-1)\left(\ell-\left(\frac{\Delta_K}{\ell}\right)\right)}\right). \tag{4}$$

The factor $F_4(r,K)$ is not relevant to our discussion, and we mention only that, uniformly in r and K, one has $|F_4(r,K)| \leq 4$.

To write the Koblitz constant [12], we define, for any positive integer n, the subset

$$\Phi_n := \{g \in GL_2(\mathbb{Z}/n\mathbb{Z}) : \det(1-g) \in (\mathbb{Z}/n\mathbb{Z})^*\}. \tag{5}$$

Then we have

$$C_{E,\text{prime}} = \prod_{\ell} \frac{|G_\ell(E) \cap \Phi_\ell|/|G_\ell(E)|}{1-1/\ell}.$$

Note that (c.f. [5, Proposition 3.10]) one has

$$C_{E,\text{prime}} = \prod_{\ell | 6\Delta_E} \frac{|G_\ell(E) \cap \Phi_\ell|/|G_\ell(E)|}{1-1/\ell} \cdot \prod_{\ell \nmid 6\Delta_E} \left(1 - \chi(\ell) \frac{\ell^2-\ell-1}{(\ell-\chi(\ell))(\ell-1)^2}\right),$$

where χ is the quadratic character corresponding to the quadratic field K.

Finally, the cyclicity constant has the same definition on the CM and non-CM case, namely

$$C_{E,\text{cyclic}} = \sum_{n \geq 1} \frac{\mu(n)}{[\mathbb{Q}(E[n]) : \mathbb{Q}]}. \tag{6}$$

3.2 The non-CM case and the average constants

In each non-CM case, we will write constant C_E in the form

$$C_E = f(m_E, G_{m_E}(E)) \cdot \prod_{\ell \nmid m_E} f(\ell, GL_2(\mathbb{Z}/\ell\mathbb{Z})),$$

where $f(n, G)$ is some function of the level n and the subgroup $G \leq GL_2(\mathbb{Z}/n\mathbb{Z})$, and where m_E is a positive integer depending on the torsion representation attached to E. We proceed to describe m_E.

Another way to phrase Notation 10 is to say that there is a group homomorphism

$$\varphi_{E,n} : G_{\mathbb{Q}} \to GL_2(\mathbb{Z}/n\mathbb{Z}),$$

defined by letting the absolute Galois group $G_{\mathbb{Q}} := \text{Gal}\,(\overline{\mathbb{Q}}/\mathbb{Q})$ act on the n-torsion points of E, and we are denoting the image of $\varphi_{E,n}$ by $G_n(E)$. Taking the inverse limit of the $\varphi_{E,n}$ over positive integers n (ordered by divisibility), one obtains a continuous group homomorphism

$$\varphi_E : G_{\mathbb{Q}} \to GL_2(\hat{\mathbb{Z}}).$$

(Here $\hat{\mathbb{Z}} := \lim_{\leftarrow} \mathbb{Z}/n\mathbb{Z} = \prod_p \mathbb{Z}_p$.) Serre [16] showed that, when E has no complex multiplication, the image of this representation is open, i.e. that

$$[GL_2(\hat{\mathbb{Z}}) : \varphi_E(G_{\mathbb{Q}})] < \infty.$$

Equivalently, there is some positive integer level m_E so that, if

$$\pi : GL_2(\hat{\mathbb{Z}}) \to GL_2(\mathbb{Z}/m_E\mathbb{Z})$$

is the natural projection, one has

$$\varphi_E(G_{\mathbb{Q}}) = \pi^{-1}(G_{m_E}(E)). \tag{7}$$

For a non-CM curve E over $\mathbb{Q}$, let us denote by m_E the smallest positive integer such that the above equation holds. In particular, m_E has the property that, for m_1 dividing m_E and m_2 coprime to m_E one has

$$G_{m_1 m_2}(E) \simeq G_{m_1}(E) \times GL_2(\mathbb{Z}/m_2\mathbb{Z}). \tag{8}$$

In order to write the Lang-Trotter constant $C_{E,r}$, we follow the notation in [13]: for $G \subseteq GL_2(\mathbb{Z}/n\mathbb{Z})$ any subgroup, let

$$G_r := \{g \in G \,:\, \operatorname{tr} g \equiv r \mod n\}.$$

Then,

$$\begin{aligned} C_{E,r} =& \frac{2}{\pi} \cdot \frac{m_E |G_{m_E}(E)_r|}{|G_{m_E}(E)|} \cdot \prod_{\ell \nmid m_E} \frac{\ell |GL_2(\mathbb{Z}/\ell\mathbb{Z})_r|}{|GL_2(\mathbb{Z}/\ell\mathbb{Z})|} \\ =& \frac{2}{\pi} \cdot \frac{m_E |G_{m_E}(E)_r|}{|G_{m_E}(E)|} \cdot \prod_{\substack{\ell \mid r \\ \ell \nmid m_E}} \left(1 + \frac{1}{\ell^2 - 1}\right) \cdot \prod_{\substack{\ell \nmid r \\ \ell \nmid m_E}} \left(1 - \frac{1}{(\ell-1)(\ell^2-1)}\right), \end{aligned}$$

where m_E is as in (7). On the other hand, the average constant in (1) is

$$C_r = \frac{2}{\pi} \cdot \prod_{\ell \mid r} \left(1 + \frac{1}{\ell^2 - 1}\right) \cdot \prod_{\ell \nmid r} \left(1 - \frac{1}{(\ell-1)(\ell^2-1)}\right).$$

The Koblitz constant (as refined by Zywina in [19]) is given by

$$\begin{aligned} C_{E,\text{prime}} =& \frac{|G_{m_E}(E) \cap \Phi_{m_E}|/|G_{m_E}(E)|}{\prod_{\ell \mid m_E}(1 - 1/\ell)} \cdot \prod_{\ell \nmid m_E} \frac{|GL_2(\mathbb{Z}/\ell\mathbb{Z}) \cap \Phi_\ell|/|GL_2(\mathbb{Z}/\ell\mathbb{Z})|}{(1 - 1/\ell)} \\ =& \frac{|G_{m_E}(E) \cap \Phi_{m_E}|/|G_{m_E}(E)|}{\prod_{\ell \mid m_E}(1 - 1/\ell)} \cdot \prod_{\ell \nmid m_E} \left(1 - \frac{\ell^2 - \ell - 1}{(\ell-1)^3(\ell+1)}\right). \end{aligned}$$

In this case the average constant in (2) is given by

$$C_{\text{prime}} = \prod_{\ell} \left(1 - \frac{\ell^2 - \ell - 1}{(\ell-1)^3(\ell+1)}\right)$$

Finally, the cyclicity constant is given by

$$C_{E,\text{cyclic}} = \sum_{k \geq 1} \frac{\mu(k)}{|G_k(E)|} = \left(\sum_{k \mid m_E} \frac{\mu(k)}{|G_k(E)|}\right) \cdot \prod_{\ell \nmid m_E} \left(1 - \frac{1}{\ell(\ell-1)^2(\ell+1)}\right),$$

the second equality coming from (8) and the fact that any square-free integer k may be decomposed as $k = k_1 \cdot k_2$, where $k_1 \mid m_E$ and $(k_2, m_E) = 1$. The average constant in (3) is

$$C_{\text{cyclic}} = \prod_{\ell} \left(1 - \frac{1}{\ell(\ell-1)^2(\ell+1)}\right).$$

We first note that if any non-CM elliptic curve E were to satisfy $m_E = 1$ (i.e. if φ_E were surjective), then we would have $C_E = C$. However, as observed by Serre, *no* elliptic curve over $\mathbb{Q}$ has $m_E = 1$. The main difficulty in proving Theorem 6 is tracking the variation of m_E with E. To prove the theorem, we will focus on a density one subset of curves E for which m_E is essentially equal to the square-free part of the discriminant of E. These curves are called *Serre curves* and will be discussed in detail in the next section.

The proof of Theorem 6 will proceed as follows. We will decompose the sum

$$\sum_{E \in \mathcal{C}} |C_E - C|^k = \sum_{\substack{E \in \mathcal{C} \\ E \text{ is a Serre curve}}} |C_E - C|^k + \sum_{\substack{E \in \mathcal{C} \\ E \text{ is not a Serre curve}}} |C_E - C|^k.$$

In Section 5, we will show that, for each $\varepsilon > 0$, one has

$$\frac{1}{|\mathcal{C}|} \sum_{\substack{E \in \mathcal{C} \\ E \text{ is a Serre curve}}} |C_E - C|^k \ll_{k,\varepsilon} A^{\varepsilon} \cdot \left(\frac{\log B}{B}\right)^{k/(k+1)},$$

proving Theorem 9. In Section 6 we will show that, assuming an affirmative answer to Question 5, one has

$$\frac{1}{|\mathcal{C}|} \sum_{\substack{E \in \mathcal{C} \\ E \text{ is not a Serre curve}}} |C_E - C|^k \ll \frac{\log^{3k+\gamma}(A^3 + B^2)}{\sqrt{\min\{A, B\}}},$$

concluding the proof of Theorem 6.

4 Serre curves

Serre [16] observed that although the torsion representation φ_E has finite index in $GL_2(\hat{\mathbb{Z}})$, it is never surjective when the base field is $\mathbb{Q}$. For each elliptic curve E over $\mathbb{Q}$, there is an index two subgroup $H_E \subseteq GL_2(\hat{\mathbb{Z}})$ with $\varphi_E(G_{\mathbb{Q}}) \subseteq H_E$. (We will presently describe this subgoup.)

Definition 11. *An elliptic curve E over $\mathbb{Q}$ is a* Serre curve *if $\varphi_E(G_{\mathbb{Q}}) = H_E$.*

In other words, a Serre curve is an elliptic curve whose torsion representation has image which is "as large as possible."

We now describe the subgroup H_E: Let $\Delta = \Delta_E$ denote the discriminant of E and Δ_{sf} its square-free part, i.e. Δ_{sf} is the unique square-free integer so that

$$\frac{\Delta}{\Delta_{sf}} \in \mathbb{Q}^2.$$

The subgroup H_E will be the full preimage under the canonical surjection

$$\pi : GL_2(\hat{\mathbb{Z}}) \to GL_2(\mathbb{Z}/M\mathbb{Z})$$

of a particular index two subgroup of $GL_2(\mathbb{Z}/M\mathbb{Z})$ for a certain level M. If $\Delta_{sf} = 1$, then every element of $G_2(E)$ must be an even permutation, where we embed $G_2(E)$ into the symmetric group S_3 by representing it on the non-identity 2-torsion points. In this case $M = 2$ and we take H_E to be $\pi^{-1}(A_3)$, where A_3 is the alternating group. Otherwise, the quadratic field $\mathbb{Q}(\sqrt{\Delta})$, being a non-trivial abelian extension of $\mathbb{Q}$, is contained in a cyclotomic extension. Let D_E be the smallest positive integer for which

$$\mathbb{Q}(\sqrt{\Delta}) \subseteq \mathbb{Q}(\zeta_{D_E}).$$

In fact,

$$D_E = \begin{cases} |\Delta_{sf}(E)| & \text{if } \Delta_{sf}(E) \equiv 1 \mod 4 \\ 4|\Delta_{sf}(E)| & \text{otherwise} \end{cases},$$

where $\Delta_{sf}(E)$ is the squarefree part of the discriminant of E. Then we define

$$M_E = \begin{cases} 2|\Delta_{sf}(E)| & \text{if } \Delta_{sf}(E) \equiv 1 \mod 4 \\ 4|\Delta_{sf}(E)| & \text{otherwise} \end{cases} \tag{9}$$

to be the least common multiple of 2 and D_E, so that $\mathbb{Q}(E[M_E])$ is the compositum of $\mathbb{Q}(E[2])$ and $\mathbb{Q}(E[D_E])$. Since

$$\mathbb{Q}(\sqrt{\Delta}) \subseteq \mathbb{Q}(E[2]) \cap \mathbb{Q}(E[D_E]),$$

the corresponding Galois group $G_{M_E}(E) := \mathrm{Gal}(\mathbb{Q}(E[M_E])/\mathbb{Q})$ must be a proper subgroup of $GL_2(\mathbb{Z}/M_E\mathbb{Z})$. In particular, the character on $GL_2(\mathbb{Z}/M_E\mathbb{Z})$ which describes the action on $\sqrt{\Delta}$ of an element considering the tower of fields

$$\mathbb{Q}(\sqrt{\Delta}) \subseteq \mathbb{Q}(\zeta_{D_E}) \subseteq \mathbb{Q}(E[M_E])$$

is given by

$$\sigma : \sqrt{\Delta} \mapsto \left(\frac{\Delta_{sf}(E)}{\det \sigma}\right)\sqrt{\Delta}.$$

On the other hand, the inclusion

$$\mathbb{Q}(\sqrt{\Delta}) \subseteq \mathbb{Q}(E[2]) \subseteq \mathbb{Q}(E[M_E])$$

demands that for each $\sigma \in G_{M_E}(E)$,

$$\sigma : \sqrt{\Delta} \mapsto \varepsilon(\sigma)\sqrt{\Delta},$$

where ε denotes the projection $GL_2(\mathbb{Z}/M_E\mathbb{Z}) \to GL_2(\mathbb{Z}/2\mathbb{Z})$ followed by the signature on $GL_2(\mathbb{Z}/2\mathbb{Z}) \simeq S_3$. Thus we see that, with the notation as defined,

$$G_{M_E}(E) \subseteq \ker\left(\varepsilon(\cdot)\left(\frac{\Delta_{sf}(E)}{\det(\cdot)}\right)\right) \subseteq GL_2(\mathbb{Z}/M_E\mathbb{Z}). \tag{10}$$

In this case we therefore make the definition

$$H_E = \pi^{-1}\left(\ker\left(\varepsilon(\cdot)\left(\frac{\Delta_{sf}(E)}{\det(\cdot)}\right)\right)\right).$$

Note that M_E always divides m_E, and if we interpret $\left(\frac{\Delta_{sf}(E)}{\det(\cdot)}\right)$ to be the trivial character in case $\Delta_{sf} = 1$, we have

$$E \text{ is a Serre curve } \iff m_E = M_E \text{ and } G_{M_E}(E) = \ker\left(\varepsilon(\cdot)\left(\frac{\Delta_{sf}(E)}{\det(\cdot)}\right)\right). \tag{11}$$

One shows easily that, for d a proper divisor of M_E and π denoting the natural projection $GL_2(\mathbb{Z}/M_E\mathbb{Z}) \to GL_2(\mathbb{Z}/d\mathbb{Z})$, one has

$$\pi\left(\ker\left(\varepsilon\cdot\left(\frac{\Delta_{sf}(E)}{\det(\cdot)}\right)\right)\right) = GL_2(\mathbb{Z}/d\mathbb{Z}).$$

Thus in particular, when E is a Serre curve and $d \mid M_E$, one has

$$G_d(E) = \begin{cases} \ker\left(\varepsilon\cdot\left(\frac{\Delta_{sf}(E)}{\det(\cdot)}\right)\right) & \text{if } d = M_E \\ GL_2(\mathbb{Z}/d\mathbb{Z}) & \text{otherwise.} \end{cases} \tag{12}$$

5 The average over Serre curves

We will now show that for each $\varepsilon > 0$, one has

$$\frac{1}{|\mathcal{C}|}\sum_{\substack{E\in\mathcal{C}\\ E \text{ is a Serre curve}}} |C_E - C|^k \quad \ll_{k,\varepsilon} \quad A^{\varepsilon}\cdot\left(\frac{\log B}{B}\right)^{k/(k+1)}. \tag{13}$$

5.1 The constants associated to Serre curves

In this section, we will explicitly compute the constants $C_{E,r}$, $C_{E,\text{prime}}$ and $C_{E,\text{cyclic}}$ for E a Serre curve. For the Lang-Trotter constant $C_{E,r}$, we must fix some notation. First define the exponent $k \in \{1,2,3\}$ and the odd integer W by

$$W := \frac{\Delta_{sf}}{(\Delta_{sf},2)} \qquad \text{and} \qquad k := \begin{cases} 1 & \text{if } \Delta_{sf} \equiv 1 \mod 4 \\ 2 & \text{if } \Delta_{sf} \equiv 3 \mod 4 \\ 3 & \text{if } \Delta_{sf} \equiv 2 \mod 4. \end{cases}$$

In other words, we have

$$M_E =: 2^k \cdot W, \tag{14}$$

where M_E is as in (9). When 2^{k-1} divides r, we further define the symbol $\delta(\Delta_{sf}, r) \in \{\pm 1\}$ by

$$\delta(\Delta_{sf}, r) := (-1)^{\omega\left(\frac{W}{(W,r)}\right)+\frac{W+1}{2}+\frac{r}{2^{k-1}}}\cdot\chi_4\left(-\frac{\Delta_{sf}}{2}\right), \tag{15}$$

where we make the convention that $\chi_4(x) = 1$ if $x \notin \mathbb{Z}$.

Proposition 12. *Suppose that E is an elliptic curve over $\mathbb{Q}$ which is a Serre curve. Then*

$$C_{E,r} = \begin{cases} C_r \left(1 + \delta(\Delta_{sf}, r) \cdot \frac{M_E \cdot 2^{k-1} \cdot \varphi((W,r))}{|GL_2(\mathbb{Z}/M_E\mathbb{Z})_r|}\right) & \text{if } 2^{k-1} \mid r \\ C_r & \text{otherwise,} \end{cases} \tag{16}$$

$$C_{E,prime} = \begin{cases} C_{prime} \left(1 + \prod_{p|\Delta_{sf}} \frac{1}{p^3 - 2p^2 - p + 3}\right) & \text{if } \Delta_{sf} \equiv 1 \mod 4 \\ C_{prime} & \text{otherwise} \end{cases}, \tag{17}$$

and

$$C_{E,cyclic} = \begin{cases} C_{cyclic} \left(1 + \frac{\mu(M_E)}{\prod_{\ell | M_E} (|GL_2(\mathbb{Z}/\ell\mathbb{Z})| - 1)}\right) & if \Delta_{sf} \equiv 1 \mod 4 \\ C_{cyclic} & \text{otherwise} \end{cases}. \tag{18}$$

The proof of the proposition will require the use of some technical lemmas. We now describe the set-up of the first of these lemmas. Let M be any positive integer and recall the isomorphism of the Chinese remainder theorem:

$$GL_2(\mathbb{Z}/M\mathbb{Z}) \simeq \prod_{p^k || M} GL_2(\mathbb{Z}/p^k\mathbb{Z}), \qquad x \mapsto (x_{p^k}) \tag{19}$$

Suppose that $X_M \subseteq GL_2(\mathbb{Z}/M\mathbb{Z})$ is any subset which, under (19), satisfies

$$X_M \simeq \prod_{p^k || M} X_{p^k},$$

where X_{p^k} denotes the projection of X_M onto the p^k-th factor. Suppose further that, for each prime p dividing M we have a group homomorphism

$$\psi_{p^k} : GL_2(\mathbb{Z}/p^k\mathbb{Z}) \longrightarrow \{\pm 1\},$$

and write

$$\psi_M : GL_2(\mathbb{Z}/M\mathbb{Z}) \longrightarrow \{\pm 1\}, \qquad \psi_M(x) := \prod_{p^k || M} \psi_{p^k}(x_{p^k}).$$

Lemma 13. *With notation as just outlined, we have*

$$|\psi_M^{-1}(\pm 1) \cap X_M| \;=\; \frac{1}{2}\left(|X_M| \;\pm\; \prod_{p^k || M} \left(|\psi_{p^k}^{-1}(1) \cap X_{p^k}| - |\psi_{p^k}^{-1}(-1) \cap X_{p^k}|\right)\right).$$

Proof. We begin by noting that

$$\begin{aligned} \left|\psi_M^{-1}(\pm 1) \cap X_M\right| &= \sum_{\substack{(s_p)_{p|M} \\ \prod s_p = \pm 1}} \prod_{p^k || M} \left|\psi_{p^k}^{-1}(s_p) \cap X_{p^k}\right| \\ &= \sum_{\substack{(s_p)_{p|M} \\ \prod s_p = \pm 1}} \prod_{p^k || M} \left(F_1(p^k) + s_p F_{-1}(p^k)\right), \end{aligned}$$

where

$$F_1(p^k) := \frac{1}{2}|X_{p^k}| \quad \text{and} \quad F_{-1}(p^k) := \frac{1}{2}\left(|\psi_{p^k}^{-1}(1) \cap X_{p^k}| - |\psi_{p^k}^{-1}(-1) \cap X_{p^k}|\right).$$

Here our notation is meant to indicate that the sum runs over all $\omega(M)$-tuples $(s_p)_{p|M}$ of ± 1's which satisfy $\prod_{p|M} s_p = \pm 1$. Expanding the product and reversing summation, we obtain

$$\left|\psi_M^{-1}(\pm 1) \cap X_M\right| \quad = \quad \sum_{(t_p)_{p|M}} \prod_{p^k||M} F_{t_p}(p^k) \left(\sum_{\substack{(s_p)_{p|M} \\ \prod s_p = \pm 1}} \left(\prod_{\substack{p|M \\ t_p=-1}} s_p \right) \right), \quad (20)$$

where now (t_p) runs over *all* $\omega(M)$-tuples of ± 1's. Now we show that, for all tuples (t_p) except $(t_p) \in \{(1,1,\ldots,1),(-1,-1,\ldots,-1)\}$, the innermost sum is equal to zero. For suppose that

$$\{p : p \mid M, t_p = 1\} \neq \emptyset \neq \{p : p \mid M, t_p = -1\},$$

and fix a prime p_1 with $t_{p_1} = 1$ and a prime p_2 with $t_{p_2} = -1$. For a tuple (s_p), define its dual $(\hat{s}_p)$ by

$$\hat{s}_{p_1} = -s_{p_1}, \quad \hat{s}_{p_2} = -s_{p_2}, \quad \text{and} \quad \hat{s}_p = s_p \quad (p \notin \{p_1, p_2\}).$$

Noting that

$$\prod_{p|M} s_p = \prod_{p|M} \hat{s}_p \quad \text{and} \quad \prod_{\substack{p|M \\ t_p=-1}} s_p + \prod_{\substack{p|M \\ t_p=-1}} \hat{s}_p = 0,$$

we see that, except when $(t_p) \in \{(1,1,\ldots,1),(-1,-1,\ldots,-1)\}$, the innermost sum in (20) vanishes. Thus,

$$\left|\psi_M^{-1}(\pm 1) \cap X_M\right| \quad = \quad \frac{1}{2}\left(\prod_{p^k||M} F_1(p^k) \pm \prod_{p^k||M} F_{-1}(p^k) \right),$$

proving the lemma. □

Proof of (16). If E is a non-CM curve then

$$\frac{C_{E,r}}{C_r} \quad = \quad \frac{m_E |G_{m_E}(E)_r|}{|G_{m_E}(E)|} \cdot \prod_{\ell | m_E} \frac{|GL_2(\mathbb{Z}/\ell\mathbb{Z})|}{\ell |GL_2(\mathbb{Z}/\ell\mathbb{Z})_r|}.$$

Thus, when E is a Serre curve, we use (11) and (14) to write

$$\frac{C_{E,r}}{C_r} \quad = \quad \frac{2^k W}{2W} \cdot \frac{2\left|\left(\ker\left(\varepsilon \cdot \left(\frac{\Delta_{sf}}{\det(\cdot)}\right)\right)\right)_r\right|}{|GL_2(\mathbb{Z}/M_E\mathbb{Z})_r|} \cdot \frac{|GL_2(\mathbb{Z}/2^k\mathbb{Z})_r|}{|GL_2(\mathbb{Z}/2\mathbb{Z})_r|} \cdot \frac{|GL_2(\mathbb{Z}/2\mathbb{Z})|}{|GL_2(\mathbb{Z}/2^k\mathbb{Z})|}.$$

Now we use the following corollary of Lemma 17 below.

Corollary 14. *For $k \in \{1,2,3\}$, we have*

$$|GL_2(\mathbb{Z}/2^k\mathbb{Z})_r| = \begin{cases} 2^{3k-1} & \text{if } r \text{ is even} \\ 2^{3k-2} & \text{if } r \text{ is odd.} \end{cases}$$

The corollary, together with $|GL_2(\mathbb{Z}/2^k\mathbb{Z})| = 3 \cdot 2^{4k-3}$, implies that

$$\frac{C_{E,r}}{C_r} \quad = \quad \frac{2\left|\left(\ker\left(\varepsilon \cdot \left(\frac{\Delta_{sf}}{\det(\cdot)}\right)\right)\right)_r\right|}{|GL_2(\mathbb{Z}/M_E\mathbb{Z})_r|}.$$

To evaluate $\left|\left(\ker\left(\varepsilon \cdot \left(\frac{\Delta_{sf}}{\det(\cdot)}\right)\right)\right)_r\right|$, we will apply Lemma 13 with $M = M_E$ and

$$\psi_{p^k}(\sigma) := \begin{cases} \left(\frac{\det(\sigma)}{p}\right) & \text{if } p \text{ is odd} \\ \varepsilon(\sigma) & \text{if } p^k = 2 \text{ and } \Delta_{sf} \equiv 1 \mod 4 \\ \chi_4(\det\sigma)\varepsilon(\sigma) & \text{if } p^k = 4 \text{ and } \Delta_{sf} \equiv 3 \mod 4 \\ \chi_8(\det\sigma)\varepsilon(\sigma) & \text{if } p^k = 8 \text{ and } \Delta_{sf} \equiv 2 \mod 8 \\ \chi_4(\det\sigma)\chi_8(\det\sigma)\varepsilon(\sigma) & \text{if } p^k = 8 \text{ and } \Delta_{sf} \equiv 6 \mod 8. \end{cases} \tag{21}$$

Note that we then have $\varepsilon \cdot \left(\frac{\Delta_{sf}}{\det(\cdot)}\right) = \prod_{p^k||M_E} \psi_{p^k}(\cdot)$. Thus, by Lemma 13, we have

$$\frac{C_{E,r}}{C_r} \quad = \quad 1 + \frac{\prod_{p^k||M_E}\left(|\psi_{p^k}^{-1}(1)_r| - |\psi_{p^k}^{-1}(-1)_r\right)}{|GL_2(\mathbb{Z}/M_E\mathbb{Z})_r|}. \tag{22}$$

Lemma 15. *For odd primes p, one has*

$$\psi_{p^k}(1)_r - \psi_{p^k}(-1)_r = \begin{cases} \left(\frac{-1}{p}\right)p(p-1) & \text{if } p \mid r \\ -\left(\frac{-1}{p}\right)p & \text{if } p \nmid r. \end{cases}$$

Proof of Lemma 15. For r and d modulo p, it is straightforward to show that

$$|\{g \in GL_2(\mathbb{Z}/p\mathbb{Z}) : \operatorname{tr} g = r,\ \det g = d\}| \ = \ p\left(p + \left(\frac{r^2-4d}{p}\right)\right).$$

Thus, partitioning $\psi_p^{-1}(\pm 1)_r$ by determinant shows that

$$|\psi_p^{-1}(\pm 1)_r| = \sum_{\left(\frac{d}{p}\right)=\pm 1} p\left(p + \left(\frac{r^2-4d}{p}\right)\right). \tag{23}$$

To evaluate this sum we use the following corollary of [11, Lemma 6].

Sublemma 16. *For r nonzero modulo p,*

$$\sum_{\left(\frac{d}{p}\right)=\pm 1}\left(\frac{r^2-4d}{p}\right) \ = \ -\frac{1 \pm \left(\frac{-1}{p}\right)}{2},$$

while if $r \equiv 0 \mod p$ *then*

$$\sum_{(\frac{d}{p})=\pm 1} \left(\frac{r^2-4d}{p}\right) = \pm\left(\frac{-1}{p}\right)\frac{p-1}{2}.$$

Inserting this into (23), we finish the proof of Lemma 15. □

For $p = 2$, we use the following lemma, whose proof is a straightforward calculation which we omit.

Lemma 17. *If* $\Delta_{sf} \equiv 1 \mod 4$ *then*

$$|\psi_2^{-1}(1)_0| = 1,\ |\psi_2^{-1}(-1)_0| = 3,\ |\psi_2^{-1}(1)_1| = 2, \quad \textit{and}\ |\psi_2^{-1}(-1)_1| = 0.$$

If $\Delta_{sf} \equiv 3 \mod 4$ *then*

$$|\psi_4^{-1}(1)_0| = |\psi_4^{-1}(-1)_2| = 12,\ |\psi_4^{-1}(-1)_0| = |\psi_4^{-1}(1)_2| = 20,$$

and for any odd r *modulo* 4*,*

$$|\psi_4^{-1}(\pm 1)_r| = 8.$$

If $\Delta_{sf} \equiv 2 \mod 4$ *then*

$$|\psi_8^{-1}(\pm 1)_r| = \begin{cases} 16\cdot 8 & \textit{if } r \equiv 2 \mod 4 \\ 16\cdot 4 & \textit{if } r \textit{ is odd.} \end{cases},$$

while

$$|\psi_8^{-1}(1)_0| = |\psi_8^{-1}(-1)_4| = \begin{cases} 16\cdot 9 & \textit{if } \Delta_{sf} \equiv 2 \mod 8 \\ 16\cdot 7 & \textit{if } \Delta_{sf} \equiv 6 \mod 8 \end{cases}$$

and

$$|\psi_8^{-1}(-1)_0| = |\psi_8^{-1}(1)_4| = \begin{cases} 16\cdot 7 & \textit{if } \Delta_{sf} \equiv 2 \mod 8 \\ 16\cdot 9 & \textit{if } \Delta_{sf} \equiv 6 \mod 8. \end{cases}$$

Corollary 18. *For* ψ_{2^k} *as in* (21)*, we have*

$$\psi_{2^k}(1)_r - \psi_{2^k}(-1)_r = \begin{cases} -(-1)^{r/2^{k-1}}\chi_4(-\Delta_{sf}/2)\cdot 2^{2k-1} & \textit{if } 2^{k-1} \mid r \\ 0 & \textit{otherwise,} \end{cases}$$

where here we use the convention that $\chi_4(x) = 1$ *if* x *is not an integer.*

Inserting the results of Corollary 18 and Lemma 15 into (22), we finish the proof of (16). □

Having proved (16), we now proceed to

Proof of (17). This computation may also be found in [19]. For any non-CM elliptic curve E, we have

$$\frac{C_{E,\mathrm{prime}}}{C_{\mathrm{prime}}} = \frac{|G_{m_E}(E) \cap \Phi_{m_E}|}{|G_{m_E}(E)|} \cdot \prod_{\ell | m_E} \left(\frac{|GL_2(\mathbb{Z}/\ell\mathbb{Z})|}{|\Phi_\ell|} \right).$$

If E is a Serre curve, then we have

$$\frac{C_{E,\mathrm{prime}}}{C_{\mathrm{prime}}} = \frac{2|\psi_{M_E}^{-1}(1) \cap \Phi_{M_E}|}{|\Phi_{M_E}|}. \tag{24}$$

Applying Lemma 13, we find that

$$|\psi_{M_E}^{-1}(1) \cap \Phi_{M_E}| = \frac{1}{2} \left(|\Phi_{M_E}| + \prod_{p^k || M_E} \left(|\psi_{p^k}^{-1}(1) \cap \Phi_{p^k}| - |\psi_{p^k}^{-1}(-1) \cap \Phi_{p^k}| \right) \right).$$

Lemma 19. *For p odd, one has*

$$|\Phi_p| = p\left(p^3 - 2p^2 - p + 3\right)$$

and

$$|\psi_p^{-1}(1) \cap \Phi_p| - |\psi_p^{-1}(-1) \cap \Phi_p| = p.$$

Proof of Lemma 19. The lemma follows immediately from

$$|\psi_p^{-1}(\pm 1) \cap \Phi_p| = \frac{1}{2} \cdot p\left(p^3 - 2p^2 - p + 3 \pm 1\right).$$

□

The following lemma is a straightforward calculation using the fact that

$$\Phi_{2^k} = \varepsilon^{-1}(1).$$

Lemma 20. *One has*

$$|\psi_{2^k}^{-1}(1) \cap \Phi_{2^k}| - |\psi_{2^k}^{-1}(-1) \cap \Phi_{2^k}| = \begin{cases} 2 & \text{if } k = 1 \\ 0 & \text{if } k \in \{2, 3\}. \end{cases}$$

Inserting the results of Lemmas 19 and 20 into (24), we finish the proof of (17). □

Proof of (18). We have

$$\frac{C_{E,\mathrm{cyclic}}}{C_{\mathrm{cyclic}}} = \frac{\sum_{k | m_E} \frac{\mu(k)}{|G_k(E)|}}{\prod_{\ell | m_E} \left(1 - \frac{1}{|GL_2(\mathbb{Z}/\ell\mathbb{Z})|}\right)}.$$

If E is a Serre curve then $m_E = M_E$. Note that M_E is square-free if and only if $\Delta_{sf}(E) \equiv 1 \mod 4$. Thus, if E is a Serre curve, we deduce from (12) that

$$\sum_{k|m_E} \frac{\mu(k)}{|G_k(E)|} = \begin{cases} \prod_{\ell|m_E} \left(1 - \frac{1}{|GL_2(\mathbb{Z}/\ell\mathbb{Z})|}\right) + \frac{\mu(m_E)}{|GL_2(\mathbb{Z}/m_E\mathbb{Z})|} & \text{if } \Delta_{sf} \equiv 1 \mod 4 \\ \prod_{\ell|m_E} \left(1 - \frac{1}{|GL_2(\mathbb{Z}/\ell\mathbb{Z})|}\right) & \text{otherwise.} \end{cases}$$

This proves (18). □

We have now proved (16), (17), and (18), finishing the proof of the Proposition 12.

5.2 Averaging the Serre curve constants.

Considering Proposition 12, we see that when E is a Serre curve, C_E has the form

$$C_E = C\left(1 + g(\Delta_{sf}(E))\right) \quad \text{where} \quad g(\Delta_{sf}(E)) \ll \frac{1}{\Delta_{sf}(E)}.$$

Since the discriminant of the curve $Y^2 = X^3 + aX + b$ is $-16(4a^3 + 27b^2)$, the result (13) will follow from

$$\frac{1}{4AB} \sum_{\substack{|a|\le A \\ |b|\le B \\ 4a^3+27b^2\neq 0}} \frac{1}{|(4a^3+27b^2)_{sf}|^k} \ll_\varepsilon A^\varepsilon \cdot \left(\frac{\log B}{B}\right)^{k/(k+1)}. \tag{25}$$

Let Z be a positive real number to be chosen later. Since the left hand side is bounded by

$$\frac{1}{4AB} \sum_{\substack{|a|\le A \\ |b|\le B \\ 4a^3+27b^2\neq 0 \\ |(4a^3+27b^2)_{sf}|\le Z}} 1 \quad + \quad \frac{1}{4AB} \sum_{\substack{|a|\le A \\ |b|\le B \\ |(4a^3+27b^2)_{sf}|> Z}} \frac{1}{Z^k},$$

we are reduced to proving the following lemma.

Lemma 21. *For any $\varepsilon > 0$, we have*

$$\sum_{\substack{|a|\le A \\ |b|\le B \\ 4a^3+27b^2\neq 0 \\ |(4a^3+27b^2)_{sf}|\le Z}} 1 \ll_\varepsilon \log B \cdot Z \cdot A^{1+\varepsilon}. \tag{26}$$

Proof. The proof boils down to counting ideals of bounded norm in various quadratic fields. I would like to thank R. Daileda for helpful discussions regarding this viewpoint. We wish to count the number of integer pairs $(a, b) \in [-A, A] \times [-B, B]$ which satisfy the equation

$$4a^3 + 27b^2 = dy^2,$$

where y and d are integers with $d \neq 0$ square-free and $|d| \leq Z$. Re-writing this equation as

$$x^2 - Dy^2 = 12(-a)^3,$$

where $x = 9b$ and $D = 3d$, we see that the left hand side of (26) is bounded by

$$\sum_{\substack{2<|D|\leq 3Z \\ D \text{ square-free}}} \sum_{1\leq |a|\leq A} \#\{(\alpha,\overline{\alpha}) \in \left(\mathcal{O}_{\mathbb{Q}(\sqrt{D})}\right)^2 : \alpha\cdot\overline{\alpha} = 12a^3,\ \alpha+\overline{\alpha} \leq 18B\}, \quad (27)$$

where $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ denotes the ring of integers of $\mathbb{Q}(\sqrt{D})$. We will presently transform this into counting principal ideals rather than elements up to conjugation, but in the real quadratic case we must worry about the presence of an infinite unit group. Suppose that $(\alpha,\overline{\alpha}) \in \left(\mathcal{O}_{\mathbb{Q}(\sqrt{D})}\right)^2$ is a conjugate pair satisfying

$$\alpha\cdot\overline{\alpha} = 12a^3 \quad \text{and} \quad |\alpha+\overline{\alpha}| \leq 18B.$$

Writing $\alpha = r + s\sqrt{D}$, we may assume that r and s have the same sign. Any other $\beta \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ which generates the same ideal as α is of the form $\beta = \alpha\cdot\varepsilon_D^n$, where ε_D is a fundamental unit. One can show that the number of integers n for which

$$|\alpha\cdot\varepsilon_D^n + \overline{\alpha}\cdot\overline{\varepsilon_D}^n| \leq 18B$$

is $\ll \log B$, with an absolute constant. Thus, (27) is bounded by a constant times

$$\log B \cdot \sum_{\substack{2<|D|\leq 3Z \\ D \text{ square-free}}} \sum_{1\leq a\leq A} \eta_D^{\text{princ}}(12a^3) \ \leq\ \log B \cdot \sum_{\substack{2<|D|\leq 3Z \\ D \text{ square-free}}} \sum_{1\leq a\leq A} \eta_D(12a^3),$$

where $\eta_D(m)$ (resp. $\eta_D^{\text{princ}}(m)$) is the number of integral ideals (resp. the number of *principal* ideals) in the ring $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ of norm equal to m. We will now show that

$$\eta_D(m) \leq \tau(m). \quad (28)$$

To see this, note that the set of integral ideals I of $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ of norm m is exactly

$$\{\prod_{\substack{p^{\alpha_p}||m \\ p \text{ split}}} \mathfrak{P}^i\overline{\mathfrak{P}}^{\alpha_p-i} \cdot \prod_{\substack{p^{\alpha_p}||m \\ p \text{ inert}}} (p\mathcal{O}_{\mathbb{Q}(\sqrt{D})})^{\alpha_p/2} \cdot \prod_{\substack{p^{\alpha_p}||m \\ p \text{ ramified}}} \mathfrak{P}^{\alpha_p}\},$$

where $\mathfrak{P}$ denotes a prime ideal lying over p and $0 \leq i \leq \alpha_p$. The number of such choices is

$$\eta_D(m) = \begin{cases} \prod_{\substack{p^{\alpha_p}||m \\ p \text{ split}}} (\alpha_p+1) & \text{if } p \text{ inert } \Rightarrow 2 \mid \alpha_p, \\ 0 & \text{otherwise.} \end{cases}$$

From this, (28) is immediate. Noting that $\tau(m) \ll_\varepsilon m^\varepsilon$, one sees that

$$\log B \cdot \sum_{\substack{2<|D|\le 3Z \\ D \text{ square-free}}} \sum_{1\le a\le A} \eta_D(12a^3) \ \ll_\varepsilon \ \log B \cdot Z \cdot A^{1+\varepsilon},$$

finishing the proof of Lemma 21. □

Finally, using $Z = (B/(A^\varepsilon \log B))^{1/(k+1)}$, (25) follows, and thus so does (13).

6 The average over non-Serre curves

We finally turn to proving that

$$\frac{1}{|\mathcal{C}|} \sum_{\substack{E\in\mathcal{C} \\ E \text{ is not a Serre curve}}} |C_E - C|^k \ll_k \frac{\log^{3k+\gamma}(A^3+B^2)}{\sqrt{\min\{A,B\}}}. \tag{29}$$

In the case of the cyclicity constant, one has

$$C_{E,\mathrm{cyclic}} \le 1,$$

since the constant is a density. For the other constants, we prove the following.

Lemma 22. *Fix the integer $r \in \mathbb{Z}$. If E over $\mathbb{Q}$ is an elliptic curve with CM, then*

$$C_{E,r} = O(1) \quad \text{and} \quad C_{E,prime} = O(\log(\Delta_E)).$$

If E is a non-CM elliptic curve over $\mathbb{Q}$, then we have

$$C_{E,prime} = O(\log m_E).$$

Assuming an affirmative answer to Question 5, we have

$$C_{E,r} = O(\log^3 m_E).$$

Proof. For the Lang-Trotter constant in the CM case, we see from (4) that

$$C_{E,r} \ll \prod_{\substack{\ell\neq 2 \\ \ell\mid\Delta_K}} \left(1+\frac{1}{\ell-1}\right) \cdot \prod_{\substack{\ell\neq 2 \\ \ell\nmid\Delta_K \\ \ell\mid r}} \left(1+\frac{1}{\ell-1}\right) \ll \log\Delta_K \cdot \log r,$$

by Merten's theorem. For fixed r and using the fact (c.f. [18]) that, since E is defined over $\mathbb{Q}$, K must have class number one, we conclude that $C_{E,r}$ is uniformly bounded.

For $C_{E,r}$ in the non-CM case, we reason as follows. According to [9], we may take m_E to be of the form

$$m_E = \prod_{\substack{p\in\{2,3,5\} \text{ or} \\ G(p)\subsetneq GL_2(\mathbb{Z}/p\mathbb{Z})}} p^{\alpha_p} \cdot \prod_{\substack{p\mid\Delta_E \\ p\notin\{2,3,5\} \text{ and} \\ G(p)=GL_2(\mathbb{Z}/p\mathbb{Z})}} p^{\alpha_p} =: m_1 \cdot m_2,$$

where α_p are certain exponents, independent of E. If Question 5 has an affirmative answer then m_1 is uniformly bounded, and there must be a non-trivial intersection

$$\mathbb{Q} \subsetneq \mathbb{Q}(E[m_1]) \cap \mathbb{Q}(E[m_2]) =: F,$$

whose Galois group we will denote by H:

$$H := \mathrm{Gal}\,(F/\mathbb{Q}).$$

The restriction of an automorphism to the subfield F defines group homomorphisms

$$\chi : G(m_1) \longrightarrow H, \qquad \psi : G(m_2) \longrightarrow H,$$

and the Galois group of the m_E-th division field may be identified as

$$\mathrm{Gal}\,(\mathbb{Q}(E[m_E)/\mathbb{Q}) = \{(\tau_1, \tau_2) \in G(m_1) \times G(m_2) : \chi(\tau_1) = \psi(\tau_2)\} = \ker \chi \otimes \psi^{-1}.$$

Because of basic facts about the group $GL_2(\mathbb{Z}_p)$ (c.f. [15]) one has $G(m_2) = GL_2(\mathbb{Z}/m_2\mathbb{Z})$. As observed in [15], the common quotient H of $G(m_1)$ and $GL_2(\mathbb{Z}/m_2\mathbb{Z})$ must be abelian, and since the commutator subgroup of $GL_2(\mathbb{Z}/m_2\mathbb{Z})$ is equal to $SL_2(\mathbb{Z}/m_2\mathbb{Z})$, we see that $\psi = \delta \circ \det$ for some homomorphism

$$\delta : (\mathbb{Z}/m_2\mathbb{Z})^* \longrightarrow H.$$

Considering the decomposition

$$G(m_E)_r = \left(\ker \chi \otimes \psi^{-1}\right)_r = \bigsqcup_{h \in H} \chi^{-1}(h)_r \times \det{}^{-1}(\delta^{-1}(h))_r,$$

we are led to

Lemma 23. *Fix any odd prime power p^n and integers $r \in \mathbb{Z}/p^n\mathbb{Z}$ and $d \in (\mathbb{Z}/p^n\mathbb{Z})^*$. Then we have*

$$|\{A \in M_{2\times 2}(\mathbb{Z}/p^n\mathbb{Z}) : tr(A) = r, \det(A) = d\}| \ \leq \ p^{2n}\left(1 + \frac{3}{p}\right)$$

Proof of Lemma 23. In fact, we will evaluate the left-hand side explicitly. Writing

$$r^2 - 4d =: \Delta =: p^\delta \cdot \Delta',$$

where $p \nmid \Delta'$, we will show that

$$|\{A \in M_{2\times 2}(\mathbb{Z}/p^n\mathbb{Z}) : \mathrm{tr}\,(A) = r, \det(A) = d\}| \ = \ p^{2n}\left(1 + \frac{1}{p} + f(p, \Delta)\right), \tag{30}$$

where

$$f(p,\Delta) := \begin{cases} -p^{-(n+1)/2} & \text{if } \delta = n \text{ is odd} \\ -p^{-(n+2)/2} & \text{if } \delta = n \text{ is even} \\ -\left(p^{-(\delta+1)/2} + p^{-(\delta+3)/2}\right) & \text{if } \delta < n, 2 \nmid \delta \\ \left(\left(\frac{\Delta/p^\delta}{p}\right)\left(\delta + 2 - \frac{\delta+1}{p}\right) + \delta - \frac{\delta+1}{p}\right) p^{-(\delta/2+1)} & \text{if } \delta < n, 2 \mid \delta, \end{cases}$$

where $\left(\frac{\cdot}{p}\right)$ denotes the Legendre symbol. Lemma 23 follows upon observing that

$$\left|\left(\left(\frac{\Delta/p^{\delta}}{p}\right)\left(\delta+2-\frac{\delta+1}{p}\right)+\delta-\frac{\delta+1}{p}\right)p^{-(\delta/2+1)}\right| \leq \frac{2}{p},$$

which can be proved by using elementary calculus techniques to bound the function

$$y \mapsto \frac{2}{p}-\frac{2y}{p^{y/2+1/2}}+\frac{2y}{p^{y/2+3/2}} \qquad (y \in [1,\infty)).$$

To prove (30), we reason as follows. Writing a matrix of trace r as

$$A=\begin{pmatrix} a & b \\ c & r-a \end{pmatrix},$$

we are led to ask how many solutions (a,b,c) modulo p^n there are to the equation

$$\left(a-\frac{r}{2}\right)^2 \equiv \frac{\Delta-4bc}{4} \mod p^n, \tag{31}$$

which leads us to the following two sublemmas, whose proofs are straightforward calculations.

Sublemma 24. *For any odd prime power p^n, the number N_y of solutions x modulo p^n to*

$$x^2 \equiv y \mod p^n$$

is given by

$$N_y=\begin{cases} p^{n-\lceil n/2\rceil} & \text{if } y \equiv 0 \mod p^n \\ p^m\left(1+\left(\frac{y/p^{2m}}{p}\right)\right) & \text{if } y=p^{2m}\cdot y' \text{ with } p\nmid y' \text{ and } 2m<n \\ 0 & \text{otherwise.}\end{cases}$$

Sublemma 25. *For any odd prime power p^n, the number P_y of pairs (b,c) modulo p^n satisfying*

$$4bc \equiv y \mod p^n$$

is given by

$$P_y=\begin{cases} (m+1)\cdot\varphi(p^n) & \text{if } y=p^m\cdot y' \text{ with } p\nmid y' \text{ and } m<n \\ n\cdot\varphi(p^n)+p^n & \text{if } y\equiv 0 \mod p^n.\end{cases}$$

The number of solutions (a,b,c) modulo p^n to (31) is simply

$$\sum_{y \mod p^n} N_{\Delta-y}\cdot P_y.$$

Using the two sublemmas and some calculation, we arrive at (30), proving Lemma 23. □

By Lemma 23, we see that

$$|\det{}^{-1}(\delta^{-1}(h))_r| \ll \varphi(m_2)\cdot m_2^2\cdot \prod_{p\le m_2}\left(1+\frac{1}{p}\right)^3 \le m_2^3\log^3 m_2.$$

Thus we have

$$\frac{m_E|G(m_E)_r|}{|G(m_E)|}\ll \log^3 m_2,$$

which proves the bound for $C_{E,r}$ in the non-CM case.

For the Koblitz constant in the CM case, we see that

$$C_{E,\mathrm{prime}} \ll \frac{1}{\prod_{\ell|\Delta_E}(1-1/\ell)} \ll \log(\Delta_E).$$

For $C_{E,\mathrm{prime}}$ in the non-CM case, we similarly have

$$C_{E,\mathrm{prime}} \ll \frac{1}{\prod_{\ell\le m_E}(1-1/\ell)} \ll \log m_E,$$

finishing the proof of Lemma 22. □

We now use the following result, which is a restatement of [9, Theorem 3].

Theorem 26. *Assume an affirmative answer to Question 5. Then for any non-CM elliptic curve E over $\mathbb{Q}$ we have*

$$m_E \ll \left(\prod_{p|\Delta_E} p\right)^5,$$

with an absolute constant.

Note that, for $E\in\mathcal{C}$, we have

$$\prod_{p|\Delta_E} p \le \Delta_E \ll 4A^3+27B^2,$$

and thus, we have

$$\frac{1}{|\mathcal{C}|}\sum_{\substack{E\in\mathcal{C}\\ E\text{ is not a Serre curve}}}|C_E-C|^k \ll_k \frac{\log^{3k}(A^3+B^2)}{|\mathcal{C}|}\sum_{\substack{E\in\mathcal{C}\\ E\text{ is not a Serre curve}}}1$$

We finally use the following result of [10], which in our situation may be stated as follows:

Theorem 27. *There is a $\gamma>0$ so that*

$$\sum_{\substack{E\in\mathcal{C}\\ E\text{ is not a Serre curve}}}1 \ll \frac{|\mathcal{C}|\log^\gamma(\min\{A,B\})}{\sqrt{\min\{A,B\}}},$$

with an absolute implied constant.

This implies (29), finishing the proof of Theorem 6.

References

[1] S. Baier, *The Lang-Trotter conjecture on average*, preprint.

[2] A. Balog, A. C. Cojocaru, and C. David, *Average twin prime conjecture for elliptic curves*, preprint.

[3] W. Banks and I. Shparlinski, *Sato-Tate, cyclicity, and divisibility statistics on average for elliptic curves of small height*, preprint.

[4] A. C. Cojocaru, *Cyclicity of CM elliptic curves modulo p*, Trans. Amer. Math. Soc. **355** (2003), 2651–2662.

[5] ———, *Square-free orders for CM elliptic curves modulo p*, preprint.

[6] C. David and F. Papalardi, *Average frobenius distributions of elliptic curves*, International Math. Research Notices, **4** (1999), 165–183.

[7] W. D. Duke, *Elliptic curves with no exceptional primes*, C. R. Math. Acad. Sci. Paris Sér. I **325** (1997), 813–818.

[8] E. Fouvry and M. R. Murty, *On the distribution of supersingular primes*, Canad. J. math., **48**, 81–104.

[9] N. Jones, *A bound for the "torsion conductor" of a non-CM elliptic curve*, preprint.

[10] ———, *Almost all elliptic curves are Serre curves*, preprint.

[11] ———, *Trace formulas and class number sums*, preprint.

[12] N. Koblitz, *Primality of the number of points of an elliptic curve over a finite field*, Pacific Journal of Mathematics, **131**, No. 1 (1988), 157–165.

[13] S. Lang and H. Trotter, *Frobenius distributions in GL_2-extensions.* Lecture Notes in Math. **504**, Springer-Verlag, Berlin, 1976.

[14] M. R. Murty, *On Artin's conjecture*, Journal of Number Theory **16**, no. 2 (1983), 147–168.

[15] J. -P. Serre, *Abelian l-Adic Representations and Elliptic Curves*, Benjamin, New York-Amsterdam 1968.

[16] ———, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math., 15, pp. 259 - 331.

[17] ———, *Résumé des cours de 1977-1978*, Annuaire du Collège de France 1978, 67–70, in Collected Papers, vol. III, Springer Verlag, 1986, 465–468.

[18] J. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, **151**, Springer-Verlag, New York, 1994.

[19] D. Zywina, *On Koblitz's constant*, pre-print.